Getting started

Symantec AntiVirus™ for Network Appliance™ NetCache®

Copyright © 2003 Symantec Corporation.
All rights reserved.
Printed in the U.S.A.
10/03 10199302
Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Symantec AntiVirus is a trademark of Symantec Corporation. NetApp, NetCache, and Network Appliance are registered trademarks or trademarks of Network Appliance, Inc., in the United States and other countries. Other brands and products are trademarks of their respective holder/s.

About Symantec AntiVirus for Network Appliance NetCache

Symantec AntiVirus™ version 4.3 for Network Appliance™ NetCache® provides virus scanning and repair capabilities for the Network Appliance (NetApp®) NetCache appliance. Symantec AntiVirus for Network Appliance NetCache features the Symantec AntiVirus Scan Engine, a carrier-class virus scanning and repair engine that protects users on your network from Web traffic that contains viruses. The Symantec AntiVirus Scan Engine features all of the virus-scanning technologies that are available in Symantec antivirus products, making the Symantec AntiVirus Scan Engine one of the most effective virus solutions available for detecting and preventing virus attacks.

The NetApp NetCache appliance is a caching proxy server. As the NetCache appliance retrieves requested information from the Web, it also caches a copy of the information (stores a copy on disk), and, where possible, serves multiple requests for the same Web content from the cache. NetApp NetCache clients use ICAP to communicate with the Symantec AntiVirus Scan Engine. Clients can request virus scanning and repair as a file is retrieved from the Web before it is sent to the requesting user. When a virus is found in a downloaded file and the file is repaired, the clean file is cached and forwarded to the requesting user.

What's new in version 4.3

Symantec AntiVirus version 4.3 for Network Appliance NetCache includes the following new features:

- POST transaction antivirus scanning for ICAP 1.0: Symantec AntiVirus for Network Appliance NetCache now scans files that are being posted to the Internet. The antivirus scanning and logging policies that are configured on the scan engine now also apply to POST transactions as well.
- Data trickle user comforting for ICAP: This feature prevents a user who downloads a large file from the Internet from receiving a session time-out error by trickling small amounts of the file to the user while the file is being scanned.
- Command-line scanner: The Symantec AntiVirus Scan Engine now includes a command-line scanner, which lets you send files to

be scanned for viruses via the command line. You can repair infected files and delete those that are unrepairable.

- Upgrade installation support: You now can install an upgrade to the Symantec AntiVirus Scan Engine over an existing installation (without first uninstalling the previous version). Any configuration changes and customizations that have been made are preserved during the upgrade.
- Upgraded logging features: Logging for each logging destination is activated individually by selecting a desired logging level for that destination. Selecting the logging level lets you choose the types of events for which log messages are sent to that destination. You can select a different logging level for each logging destination.
- Dynamic thread pool for antivirus scanning: The pool of scanning threads that is available to the Symantec Antivirus Scan Engine for antivirus scanning now dynamically adjusts to the load that is being processed. You can change a number of parameters to control the dynamic thread pool.

About ICAP

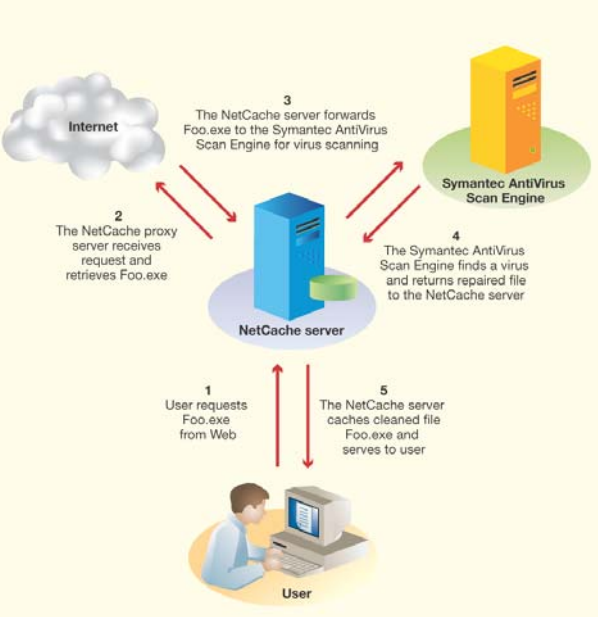
ICAP is a lightweight protocol for executing a remote procedure call on HTTP messages. ICAP is part of an evolving architecture that lets corporations, carriers, and ISPs dynamically scan, change, and augment Web content as it flows through ICAP servers. The protocol lets ICAP clients pass HTTP messages to ICAP servers for adaptation (some sort of transformation or other processing, such as virus scanning). The server executes its transformation service on messages and responds to the client, usually with modified messages. The adapted messages might be either HTTP requests or HTTP responses.

How the Symantec AntiVirus Scan Engine works with the NetApp NetCache client

Symantec AntiVirus version 4.3 for Network Appliance NetCache provides virus scanning and repair capabilities for any Network Appliance (NetApp) NetCache appliance that uses version 5.2.1R1 or later of the NetCache software. The Symantec AntiVirus Scan Engine simultaneously supports both the proprietary 0.95 implementation of ICAP and ICAP version 1.0, as presented in RFC 3507 (April 2003). The Symantec AntiVirus Scan Engine determines which version is appropriate for each request based on the header data that is provided by the NetCache appliance when it contacts the Symantec AntiVirus Scan Engine to scan a file.

A typical integration of the Symantec AntiVirus Scan Engine with a NetApp NetCache client is shown in Figure 1-1.

Figure 1-1 Integration of the Symantec AntiVirus Scan Engine with the NetCache client


Internet
3
The NetCache server forwards Foo.exe to the Symantec AntiVirus Scan Engine for virus scanning
Symantec AntiVirus Scan Engine
2
The NetCache proxy server receives request and retrieves Foo.exe
4
The Symantec AntiVirus Scan Engine finds a virus and returns repaired file to the NetCache server
NetCache server
1
User requests Foo.exe from Web
5
The NetCache server caches cleaned file Foo.exe and serves to user
User

How the scan engine determines which files to scan

The manner in which the Symantec AntiVirus Scan Engine determines whether to scan a file differs depending on which version of ICAP is used.

For ICAP 0.95, when the Symantec AntiVirus Scan Engine is contacted by the NetCache appliance to scan a file, a small amount of file data is transferred to the Symantec AntiVirus Scan Engine. (The number of bytes of data that is transferred is configured through the NetCache interface.) This data contains the file name, the HTTP header, and the first few bytes of the file to be scanned. The Symantec AntiVirus Scan Engine examines this data to determine whether to scan the file.

The Symantec AntiVirus Scan Engine first identifies the extension of the file to be scanned and then compares the extension to a configured list of extensions (on the scan engine). If the file extension is one that the scan engine is configured to scan, or if the scan engine is configured to scan all files, the Symantec AntiVirus Scan Engine

requests the remainder of the file from the NetCache client and scans it.

If the scan engine is not configured to scan the file extension or does not recognize the file extension, the Symantec AntiVirus Scan Engine examines the first few bytes of the file's contents to determine whether the file could contain a virus. Based on this examination, the scan engine might scan a file even when the extension is not listed in the extension list.

ICAP 1.0 lets the Symantec AntiVirus Scan Engine initially provide information to the NetCache client on which file types are to be scanned, based on the scan engine configuration. Based on this information, the NetCache client forwards either the entire file to the scan engine for scanning (if the file extension is one that was identified for scanning) or the first few bytes of the file to the scan engine for preview (if the file extension is unknown or is not one that was identified for scanning). The scan engine examines the first few bytes of the file to determine whether the file could contain a virus. Based on this examination, the scan engine might request and scan a file even when it is not identified for scanning.

Controlling which file types are scanned

You can control which file types the Symantec AntiVirus Scan Engine scans by using either an exclusion or an inclusion list, or you can scan all files regardless of extension. By default, the Symantec AntiVirus Scan Engine scans all file types except those contained in an exclusion list. The default exclusion list contains extensions for those file types that are not likely to contain viruses and can be excluded from scanning, but you can customize this list.

If you use either the inclusion or the exclusion list to control the file types that are scanned (rather than scanning all files), the manner in which the list is applied differs depending on which version of ICAP is being used.

See "Specifying which file types to scan" on page 6.

Disposing of infected files

When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following:

- Scan only: Deny access to the infected file, but do nothing to the infected file.
- Scan and delete: Delete all infected files, including those contained in archive files, without attempting repair.
- Scan and repair files: Attempt to repair infected files and deny access to unrepairable files, but do nothing to files that cannot be repaired.
- Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.

Alerting users when infected files cannot be repaired

You can configure the Symantec AntiVirus Scan Engine to display an HTML text message when a requested file is blocked. (Access to a file is blocked by the NetApp NetCache appliance when the file contains a virus and cannot be repaired.) The default HTML text file indicates that access is denied because the file contains a virus. You can customize the text that is displayed by editing this file or by substituting an alternate file.

See "Editing the ICAP access denied message" on page 8.

Providing user comforting

When a user attempts to download an extremely large or complex file from the Internet, antivirus scanning can cause a delay during which the requesting browser (and thus the user) receives no feedback on the progress of the download. The data trickle feature lets you provide users with a quick download response and avoid potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete.

Warning: Using the data trickle feature can compromise antivirus integrity. Before enabling this feature, ensure that you have read and understand all of the risks.

See "Enabling data trickle" on page 5.

Preparing for installation

To interface with the Symantec AntiVirus Scan Engine, the NetApp NetCache appliance must use version 5.2.1R1 or later of the NetCache software to support ICAP version 0.95 or 1.0. Before you install the scan engine, ensure that the NetApp NetCache appliance meets this requirement.

Ensure that the computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure the NetApp NetCache appliance to work with it.

Configuring the Symantec AntiVirus Scan Engine to use ICAP

The Symantec AntiVirus Scan Engine must be configured to use ICAP as the communication protocol. You can select ICAP at installation, or you can change the protocol through the administrative interface. Once you have selected ICAP, you must configure several ICAP-specific options.

If you are installing the Symantec AntiVirus Scan Engine, see "Selecting ICAP at installation" on page 4.

If the Symantec AntiVirus Scan Engine is already installed and another protocol is in use, see "Configuring the ICAP-specific options" on page 4.

Selecting ICAP at installation

This section includes only those installation steps that are specific to ICAP. For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

To select ICAP at installation

1. In the Symantec AntiVirus Scan Engine Setup dialog box, under Protocol type, click **ICAP**.
2. Continue with the installation.
   For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Configuring the ICAP-specific options

After you install the Symantec AntiVirus Scan Engine, you can configure several settings that are specific to the ICAP protocol via the Symantec AntiVirus Scan Engine administrative interface. If the Symantec AntiVirus Scan Engine has already been configured to use another protocol, you also can change the protocol via the administrative interface.

For more information about accessing the administrative interface, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Note: If you change to ICAP from the RPC protocol through the Symantec AntiVirus Scan Engine administrative interface, you must manually stop and restart the service (rather than clicking Restart on the administrative interface).

Table 1-1 describes the protocol-specific options for ICAP.

Table 1-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address.
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number greater than 1024 that is not in use by any other program or service. If you are installing more than one instance of the Symantec AntiVirus Scan Engine on a single computer, each scan engine service must have a unique port number.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains a virus. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you edit the existing file, you do not have to change this setting. See "Editing the ICAP access denied message" on page 8.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Deny access to the infected file, but do nothing to the infected file. ■ Scan and delete: Delete all infected files, including those contained in archive files, without attempting repair. ■ Scan and repair files: Attempt to repair infected files and deny access to unrepairable files, but do nothing to files that cannot be repaired. ■ Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.

Table 1-1 Protocol-specific options for ICAP

Option	Description
Data trickle	When a user attempts to download an extremely large or complex file from the Internet, antivirus scanning can cause a delay during which the requesting browser (and thus the user) receives no feedback on the progress of the download. You can use the data trickle feature to provide users with a quicker download response and avoid potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete. See "Enabling data trickle" on page 5.

To configure the ICAP-specific options

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.
   The configuration settings are displayed for the selected protocol.
3. Under ICAP Protocol Configuration, in the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
4. In the Port number box, type the TCP/IP port number that the NetApp NetCache client uses to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.
5. In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.
6. In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete. If you plan to use the data trickle feature, you must select Scan only.
7. Click **Confirm Changes** to save the configuration.
8. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
     You must stop and restart the service manually if you have changed to ICAP from RPC through the administrative interface (rather than selecting ICAP at installation).
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Enabling data trickle

When a user attempts to download an extremely large or complex file from the Internet, a period of time elapses while antivirus scanning takes place during which the browser (and thus the user) receives no feedback on the progress of the download. Without feedback, the user might try to click the browser Refresh button several times even though the download is working properly. In some instances, the browser can time out waiting for the scan to complete. The Symantec AntiVirus Scan Engine data trickle feature provides users with a quicker download response and avoids potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete.

Data trickling is available for versions 0.95 and 1.0 of ICAP. The ICAP scan policy must be set to Scan only when data trickle is enabled. (When you enable data trickle, the ICAP scan policy is automatically reset to Scan only.) In the Scan only configuration, infected files cannot be deleted or repaired.

Warning: Using data trickle can compromise antivirus integrity. Before enabling this feature, ensure that you have read and understand all of the risks.

How data trickle works

When a user downloads a file, the Symantec AntiVirus Scan Engine stores a copy of the requested file in a buffer and begins the scanning process. While the copy is being scanned, a small portion of the original, unscanned file is sent to the user via the client application. The trickled data triggers the File Download or Save File As dialog box, which provides the user with a quicker download response.

After the user enters a file location and clicks Save in the File Download or Save File As dialog box, the file is trickled to the user in small amounts at regular intervals until the scan is complete to prevent the browser from timing out.

The browser indicates how much of the file has been trickled.

If no virus is detected during the scan, data trickling stops, and the remainder of the file is sent to the user.

If a virus is detected, data trickling stops, and no additional data is sent to the user. The user receives no notification that the file might be incomplete or that it might contain a virus. (Symantec AntiVirus Scan Engine logging regarding virus detection functions normally during data trickling. A log message about the virus detection is sent to all active logging destinations.)

Note: Data trickling is not invoked during scanning of POST transaction data.

Warnings and limitations about data trickle

Enabling data trickle can compromise antivirus integrity. Symantec does not recommend using the data trickle feature for the following reasons:

- The data that is trickled to the user might contain a virus.

  Note: If you enable data trickle, you should install an antivirus program such as Symantec AntiVirus Corporate Edition that provides real-time virus scanning. If the trickled data is infected, the real-time virus scanning feature will detect the virus immediately.

- For FTP downloads that use optimizers, when a broken connection is detected, the optimizer resumes the download from the point at which the disconnection occurred. This results in downloading the remainder of the file and possibly reconstructing an infected file.
- ICAP requires that a return code message be included in the first line of the file header. When data trickling begins, ICAP return code 200 (OK) is embedded in the trickled data file. Because the file has not been scanned, this message might be inaccurate. The trickled data file might contain a virus.
- When data trickling is enabled, the ICAP scan policy is set to Scan only. You cannot configure your scanning policy to repair or delete infected files when data trickle is enabled.
- The user receives no notification that the trickled data file is incomplete or infected.

To enable data trickle

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, check **Enable Trickle**.
   Data trickling is disabled by default.
3. In the Trickle timeout box, type the number of seconds that the scan process will run before data trickling begins.
   Data trickling is not invoked if scanning is complete before the trickle time-out elapses. The default setting is 5 seconds. The maximum setting is 86,400 seconds (24 hours).
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Specifying which file types to scan

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in a prepopulated exclusion list. The default exclusion list contains those file types that are unlikely to contain viruses, but you can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those file types that are specifically listed in an inclusion list are scanned; thus, with an inclusion list, there is an almost limitless number of possible file extensions that are not scanned. For this reason, the inclusion list is not prepopulated, but you can choose to populate this list.

If you use either the inclusion or the exclusion list to control the file types that are scanned (rather than scanning all files), the manner in which the list is applied differs depending on which version of ICAP is being used:

- ICAP version 1.0: The inclusion or exclusion list is used by the Symantec AntiVirus Scan Engine to determine which files to scan of those that are embedded in archival file formats (for example, .zip or .lzh files). All top-level files that are sent to the scan engine are scanned regardless of file extension.

- ICAP version 0.95: The inclusion or exclusion list applies to all files that are sent to the Symantec AntiVirus Scan Engine for scanning. The extension list is consulted for both top-level files and embedded files that are contained in archival file formats (for example, .zip or .lzh files).

Note: Exclusion and inclusion lists by definition do not scan all file types; thus, new types of viruses might not always be detected. Scanning all files regardless of extension is the most secure setting, but imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the exclusion or inclusion list.

Specify which file types to scan

You can control which file types are scanned by specifying extensions that you want to scan or that you do not want to scan, or you can scan all files regardless of extension.

To scan all files except for those with extensions that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
3. Edit the exclusion list to add extensions that you do not want to scan or to delete extensions that you want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.
4. To restore the default extension list, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.
6. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

To scan only files with extensions that are in the inclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.
3. Edit the inclusion list to add extensions that you want to scan or to delete extensions that you do not want to scan.

   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.
4. Click **Confirm Changes** to save the configuration.
5. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the Scan Engine service now.
   - Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

To scan all files regardless of extension

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.
3. Click **Confirm Changes** to save the configuration.

4 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration. If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the Scan Engine service now.
- Click **Save/No Restart** to save your changes. (Changes will not take effect until the service is restarted.)

Editing the ICAP access denied message

Access to a file is blocked by the NetApp NetCache appliance when the file contains a virus and cannot be repaired. The Symantec AntiVirus Scan Engine passes an HTML text message to the NetCache appliance to display to the user when a requested file is blocked. The default text indicates that access is denied because the file contained a virus.

You can customize the text that is displayed in one of the following ways:

- Edit the ICAP access denied HTML file.
- Specify an alternate HTML file.

For Solaris and Linux, the default location and file name of the HTML file is /opt/SYMCScan/etc/symcsinf.htm. For Windows 2000 Server/Server 2003, the default location and file name of the file is C:\Program Files\Symantec\Scan Engine\SYMCSINF.htm.

The default text that is in the ICAP access denied message is described in Table 1-2.

Table 1-2 Default text for ICAP access denied message

Default text	Description
The content you just requested had a problem and was blocked by the Symantec AntiVirus Scan Engine based on local administrator settings. Contact your local administrator for further information.	Text that is in the symcsinf.htm file, which is displayed to the user when a requested file contains a virus and cannot be repaired

To edit the ICAP access denied message

1 Locate the Symantec AntiVirus Scan Engine ICAP access denied HTML file and open it with a text editor.

2 Make your changes to the file.

3 Save the file.

4 Stop and restart the Symantec AntiVirus Scan Engine.

Configuring NetApp NetCache clients to work with the scan engine

Each NetApp NetCache client must be configured to work with the Symantec AntiVirus Scan Engine. NetApp NetCache clients should be configured in accordance with the Network Appliance documentation and should be installed and working properly before you submit files for scanning.

Supported NetApp NetCache appliances must use version 5.2.1R1 or later of the NetCache software to work with the Symantec AntiVirus Scan Engine. Configuration of the NetCache client differs depending on which version of ICAP that you are using.

See "Configuring the NetApp NetCache client to use ICAP 1.0" on page 9.

See "Configuring the NetApp NetCache client to use ICAP 0.95" on page 10.

To use either version of ICAP, you must first activate the ICAP feature on the NetCache appliance using the license key supplied by Network Appliance.

Activating the NetApp ICAP license

To use either version of ICAP with the Symantec AntiVirus Scan Engine, NetApp NetCache customers must activate the ICAP feature on the NetCache appliance with a license. The following license key, valid through June 27, 2006, has been provided to Symantec Corporation by Network Appliance, Inc., and is approved for use by all Symantec AntiVirus Scan Engine customers:

QIMCZIE

To activate the NetApp ICAP license

1 On the Setup tab, in the menu on the left, click **System > Licenses**.
The System Licenses page appears.

2 In the ICAP license box, type the following license key: **QIMCZIE**

3 Click **Commit Changes**.

Configuring the NetApp NetCache client to use ICAP 1.0

Each NetApp NetCache client must be configured to use ICAP 1.0 to communicate with the Symantec AntiVirus Scan Engine. NetApp NetCache clients should be configured in accordance with the Network Appliance documentation.

Configure the NetApp NetCache client to use ICAP 1.0

To configure the NetApp NetCache client to use ICAP 1.0, you must do the following:

- Activate the ICAP 1.0 license on the Network Appliance NetCache if you have not already done so. See "Activating the NetApp ICAP license" on page 8.
- Enable ICAP 1.0.
- Add two service farms for the Symantec AntiVirus Scan Engine, one for scanning of inbound traffic, and one for scanning of outbound traffic (POST transactions).

To enable ICAP 1.0

1. Access the NetCache console by opening the following URL:
   http://<netcacheIP:port>
   where <netcacheIP:port> is the IP address and port number for the NetCache appliance
2. Log on to the NetCache console.
3. On the Setup tab, in the menu on the left, click **ICAP**, then click **ICAP 1.0**.
4. On the General tab, check **Enable ICAP Version 1.0**.
5. Click **Commit Changes**.
   Activate the NetApp ICAP 1.0 license on the NetCache appliance if you have not already done so. An error message displays if you have not installed the ICAP license key.
   See "Activating the NetApp ICAP license" on page 8.

To add a service farm for scanning of inbound traffic

1. Access the NetCache console by opening the following URL:
   http://<netcacheIP:port>
   where <netcacheIP:port> is the IP address and port number for the NetCache appliance
2. Log on to the NetCache console.
3. On the Setup tab, in the menu on the left, click **ICAP**, then click **ICAP 1.0**.
4. On the Service Farms tab, click **New Service Farm**.
5. In the Service Farm Name box, type a name for the new service farm.
6. In the Vectoring Point list, click **RESPMOD_PRECACHE**.
7. Check **Service Farm Enable**.
8. In the Load Balancing list, click **Least Usage Based**.
9. Ensure that the Bypass on Failure check box is not checked.
10. In the Consistency list, click **Strong**.
11. Ensure that the lbw Threshold box is empty.
12. In the Services box, type the ICAP URL string for the Symantec AntiVirus Scan Engine that will provide scanning services for inbound traffic.
    Use the following format:
    icap://<scanengineIP:port>/avscanresp on
    where <scanengineIP:port> is the IP address and port number on which the Symantec AntiVirus Scan Engine listens
13. On the ACL tab, check **Enable Access Control Lists**.
14. In the HTTP ACL box, identify the access control list for the new service farm.
    Use the following format:
    ICAP<servicefarmname>any
    where <servicefarmname> is the name of the new service farm for scanning of inbound traffic
15. On the Service Farm tab, in the list of current ICAP service farms, in the Enable column, click the check box for the new service farm.
16. Click **Commit Changes**.

To add a service farm for scanning of outbound traffic

1. Access the NetCache console by opening the following URL:
   http://<netcacheIP:port>
   where <netcacheIP:port> is the IP address and port number for the NetCache appliance
2. Log on to the NetCache console.
3. On the Setup tab, in the menu on the left, click **ICAP**, then click **ICAP 1.0**.
4. On the Service Farms tab, click **New Service Farm**.
5. In the Service Farm Name box, type the name of the new service farm.

6 In the Vectoring Point list, click **REQMOD_PRECACHE**.

7 Check **Service Farm Enable**.

8 In the Load Balancing list, click **Least Usage Based**.

9 Ensure that the Bypass on Failure check box is not checked.

10 In the Consistency list, click **Strong**.

11 Ensure that the lbw Threshold box is empty.

12 In the Services box, type the ICAP URL string for the Symantec AntiVirus Scan Engine that will provide scanning services for outbound traffic.
Use the following format:
icap://<scanengineIP:port>/avscanreq on
where <scanengineIP:port> is the IP address and port number on which the Symantec AntiVirus Scan Engine listens

13 On the ACL tab, check **Enable Access Control Lists**.

14 In the HTTP ACL box, identify the access control list for the new service farm.
Use the following format:
ICAP<servicefarmname>any
where <servicefarmname> is the name of the new service farm for scanning of outbound traffic

15 On the Service Farm tab, in the list of current ICAP service farms, in the Enable column, click the check box for the new service farm.

16 Click **Commit Changes**.

Configuring the NetApp NetCache client to use ICAP 0.95

Ensure the following when you configure the NetApp NetCache client to work with the Symantec AntiVirus Scan Engine:

- The port number that is configured for the Symantec AntiVirus Scan Engine must match the ICAP URL port number that is provided to the NetApp NetCache client.
- The configured prefix size for the number of bytes that are passed to the Symantec AntiVirus Scan Engine to determine whether a file should be scanned must be set to 4 bytes (under ICAP URL Arguments).
In cases in which the Symantec AntiVirus Scan Engine does not recognize the file extension, the scan engine examines this prefix information to decide whether to scan the entire file.
- The NetApp ICAP license must be activated on the NetCache appliance so that you can use ICAP.
See "Activating the NetApp ICAP license" on page 8.
- The ICAP settings on the NetApp NetCache client must be configured according to the guidelines in Table 1-3.

Table 1-3 ICAP 0.95 settings on the NetApp NetCache client

Setting	Recommended value
ICAP 0.95 Enable	on
ICAP Service Type	respmod
ICAP URL IP address	<Symantec AntiVirus Scan Engine IP address>
ICAP URL port number	1344
ICAP URL Arguments	/respmod?preview =4

Known issues with the NetApp NetCache appliance

The NetApp NetCache appliance might occasionally time out while waiting for a reply from the Symantec AntiVirus Scan Engine when extremely large or complex files are being scanned. When a scan request times out, the NetCache appliance returns a garbled HTTP message to the requesting browser. No setting is currently available to adjust the time-out threshold on the NetApp NetCache appliance.